PI MU EPSILON: PROBLEMS AND SOLUTIONS: FALL 2020

STEVEN J. MILLER (EDITOR)

1. Problems: Fall 2020

This department welcomes problems believed to be new and at a level appropriate for the readers of this journal. Old problems displaying novel and elegant methods of solution are also invited. Proposals should be accompanied by solutions if available and by any information that will assist the editor. An asterisk (*) preceding a problem number indicates that the proposer did not submit a solution.

Solutions and new problems should be emailed to the Problem Section Editor Steven J. Miller at sjm1@williams.edu; proposers of new problems are strongly encouraged to use LaTeX. Please submit each proposal and solution preferably typed or clearly written on a separate sheet, properly identified with your name, affiliation, email address, and if it is a solution clearly state the problem number. Solutions to open problems from any year are welcome, and will be published or acknowledged in the next available issue; if multiple correct solutions are received the first correct solution will be published (if the solution is not in LaTeX, we are happy to work with you to convert your work). Thus there is no deadline to submit, and anything that arrives before the issue goes to press will be acknowledged. Starting with the Fall 2017 issue the problem session concludes with a discussion on problem solving techniques for the math GRE subject test.

Earlier we introduced changes starting with the Fall 2016 problems to encourage greater participation and collaboration. First, you may notice the number of problems in an issue has increased. Second, any school that submits correct solutions to at least two problems from the current issue will be entered in a lottery to win a pizza party (value up to $100). Each correct solution must have at least one undergraduate participating in solving the problem; if your school solves $N \geq 2$ problems correctly your school will be entered $N \geq 2$ times in the lottery. Solutions for problems in the Spring Issue must be received by October 31, while solutions for the Fall Issue must arrive by March 31 (though slightly later may be possible due to when the final version goes to press, submitting by these dates will ensure full consideration). There was no winning school this time due to the pandemic response. Also in the last issue one problem solver was accidentally omitted; Problem #1359 was also solved by Kenneth Davenport (SCI-Dallas, Dallas, PA).

Finally, in this issue we are continuing a new feature. Each year a distinguished mathematician gives the J. Sutherland Frame Pi Mu Epsilon Lecture at MathFest. In 2019 that speaker was Alice Silverberg, Distinguished Professor at the University of California, Irvine; her talk is available at , and Problem #1366 is inspired by her lecture. For 2020 the speaker was supposed to have been Florian Luca from the University of the Witwatersrand; unfortunately MathFest was cancelled due to the response to the pandemic. The abstract for his talk, *Arithmetic and Digits*, was: *In our recent paper in the Monthly (October, 2019) with*

Date: November 5, 2020.

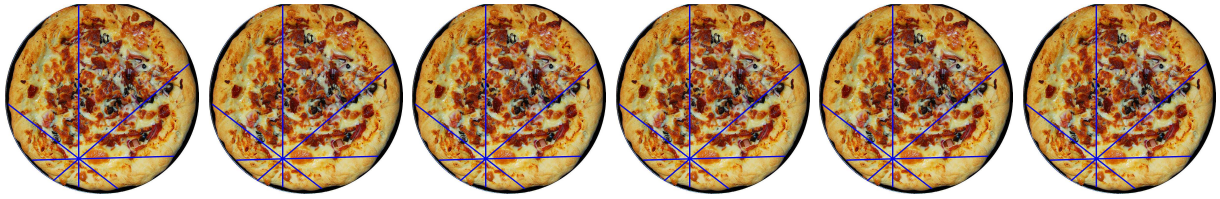

FIGURE 1. Pizza motivation; can you name the theorem that's represented here?

Pante Stănică, we looked at perfect squares which arise when concatenating two consecutive positive integers like $183184 = 428^2$ *with the smaller number to the left, or* $98029801 = 9901^2$ *with the larger number to the left. My talk will present variations on this topic with the aim of providing the audience with examples of numbers which are both arithmetically interesting (like perfect squares) while their digital representations obey some regular patterns. The examples will not be limited to perfect squares, but will also include other old friends like Fibonacci numbers and palindromes.*

NOTE: DUE TO THE CORONAVIRUS PANDEMIC AND THE CLOSURE OF COLLEGES WE ARE REPEATING THE PROBLEMS FROM SPRING 2020, AS MANY STUDENTS DID NOT HAVE A CHANCE TO WORK ON THEM WITH THEIR CLASSMATES.

#1366 (originally Spring 2020): *Proposed by Alice Silverberg (University of California, Irvine).*

Solutions to the following problems would have interesting applications to cryptography and computer security.

Problem 1: Find a way for four or more parties to create a shared secret (to use as a secret key in a symmetric key encryption scheme), with one round of broadcasts through an insecure channel.

Diffie-Hellman key agreement [2] solves this problem for two parties (see below). Pairings on elliptic curves or abelian varieties lead to a solution for three parties [3]. The problem is open for four or more parties [1].

The next problem, which was raised in [1], is a group-theoretic approach to Problem 1 that would generalize the solutions that are known in the cases of two and three parties.

Problem 2: For each (or some) fixed integer $n \geq 3$, find a large prime number p, groups G and G_T of order p, a generator g of the cyclic group G, and a function

$$e : G^n \to G_T$$

such that:

(a) it is easy to compute $e(g_1, \ldots, g_n)$ for all $g_i \in G$,

(b) $e(g_1^{a_1}, \ldots, g_n^{a_n}) = e(g_1, \ldots, g_n)^{a_1 \cdots a_n}$ for all $g_i \in G$ and all integers $a_1, \ldots, a_n$, and

(c) it is hard to compute

$$e(g, \ldots, g)^{a_1 \cdots a_{n+1}}$$

for random unknown integers $a_1, \ldots, a_{n+1}$**, even given** $g, g^{a_1}, g^{a_2}, \ldots, g^{a_{n+1}}$**.**

A solution to Problem 2 would solve Problem 1, as follows. Suppose we have $n+1$ parties. The parties publicly agree on a solution to Problem 2, namely, a prime p, groups G and G_T, a map e, and a generator g of G that satisfy (a), (b), and (c). For $i = 1, \ldots, n+1$, party i chooses a random secret integer a_i between 1 and p, computes g^{a_i}, and broadcasts that element of the group G. The shared secret is

$$e(g, \ldots, g)^{a_1 \cdots a_{n+1}} \in G_T.$$

All of the $n+1$ parties involved can compute it; the i^{th} party computes it by computing

$$e(g^{a_1}, \ldots, g^{a_{i-1}}, g^{a_{i+1}}, \ldots, g^{a_{n+1}})^{a_i},$$

which gives the desired result by (b). By (c), it is hard for anyone else to learn this shared element of the target group G_T.

For two parties, let $n = 1$, take G to be a (large) prime order subgroup of the multiplicative group of a finite field, let $G_T = G$, and let e be the identity map on G. The above protocol recovers Diffie-Hellman key agreement. Namely, Alice and Bob publicly share the prime p, the group G, and a generator g. Alice (respectively, Bob) chooses a random secret integer a (respectively, b) between 1 and p, computes g^a (respectively, g^b), and broadcasts it. The shared secret is g^{ab}, which Alice obtains by computing $(g^b)^a$ and Bob obtains by computing $(g^a)^b$. The security is based on the assumption that G was chosen so that no one else can compute g^{ab}, for random unknown a and b, even if they know g, g^a, and g^b.

Taking G to be a prime order subgroup of the group of points on a suitable elliptic curve over a finite field gives Elliptic Curve Diffie-Hellman.

For three parties, let $n = 2$. Problem 2 can be solved by taking G to be a (large) prime order subgroup of the group of points on a suitable elliptic curve E over a finite field F, and letting e be a certain (suitably modified Weil or Tate) pairing associated to E. The group G_T will be a subgroup of the multiplicative group of a certain extension field of the finite field F.

Beyond that, these problems are an area of current research.

Applications of Problem 2 to key agreement, broadcast encryption, and digital signatures were given in [1]. That paper also gave evidence that when $n \geq 3$ it might be difficult to use algebraic geometry to find a solution to Problem 2, and therefore it might be productive to look more broadly than number theory and algebraic geometry for solutions to Problems 1 and 2.

References

[1] Dan Boneh and Alice Silverberg, *Applications of multilinear forms to cryptography*, in Topics in Algebraic and Noncommutative Geometry: Proceedings in Memory of Ruth Michler, Contemporary Mathematics **324**, American Mathematical Society, Providence (2003), 71–90.

[2] Whitfield Diffie and Martin E. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory **22** (1976), 644–654.

[3] Antoine Joux, *A one round protocol for tripartite Diffie-Hellman*, Proc. ANTS IV, Lecture Notes in Computer Science **1838** (2000), 385–394.

#1367 (originally Spring 2020; note a solution to this is given below): *Proposed by Thomas Garrity, Steven J. Miller and Chenyang Sun (Williams College).*
We say a positive integer is a side-into-hypothesis number if it is both a side of a right triangle with integer lengths and the hypotenuse of a triangle with integer sides. Thus 5 is such a number, from the 3–4–5 triangle and the 5–12–13.
(a) Prove or disprove: there are infinitely many side-into-hypothesis numbers.

(b) Prove or disprove: there exists an infinite sequence of positive integers $\{x_n\}$ such that x_n is a side of a right triangle with x_{n+1} as a hypotenuse.

#1368 (originally Spring 2020): *Proposed by Steven J. Miller (Williams College).*
Consider an $n \times n$ chessboard. It is a famous (and difficult!) problem to place n queens and maximize the number of squares they do not attack; however, if we only care about the percentage in the limit then it is significantly easier. Prove that as $n \to \infty$ we can place the queens in such a way so that 100% of the squares are not attacked. Note this does not mean every square is safe; it means if $s(n)$ is the maximum number of safe squares, then $s(n)/n^2 \to 1$. Can you obtain good upper and lower bounds for $n^2 - s(n)$?

#1369 (originally Spring 2020): *Proposed by Steven J. Miller and Chenyang Sun (Williams College).*
Consider an $n \times n$ chessboard. The previous problem is greatly simplified if instead of queens we place rooks. Determine an optimal placement of n rooks to maximize the number of safe squares.

#1370 (originally Spring 2020): *Proposed by Eugen J. Ionascu (Columbus State University).*
Consider three points A, B and C chosen uniformly at random inside of the region (see Figure 1 below, the yellow region)

$$\mathcal{R}_{r,\alpha} = \{(x,y) \in \mathbb{R}^2 | x = t\cos\theta, y = t\sin\theta,\ \pi \geq |\theta| \geq \alpha, t \in [0,r]\},$$

$$\alpha \ = \ \pi a, \quad a \in [0, \tfrac{1}{2}], \quad r > 0;$$

(thus we are choosing from the uniform distribution with respect to the area). Show that the probability that the resulting triangle $\triangle ABC$ contains the origin $O(0,0)$ is equal to

$$\mathcal{P}_a \ = \ \frac{(1+a)(1-2a)^2}{4(1-a)^3}.$$

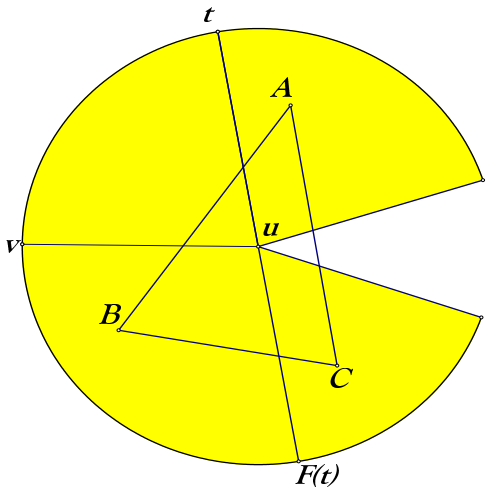

Figure 1

GRE Practice #6 (originally Spring 2020): The following is essentially the famous German Tank Problem. There are N tanks, labeled $1, 2, \ldots, N$, and k distinct serial numbers $s_1, s_2, \ldots, s_k$ are observed, with $m = \max s_i$ the largest value. If every subset of size k is equally likely, what is the best predictor for N as a function of m and k?
(a) mk (b) $m(1 + 1/k)$ (c) $m(1 - 1/k)$ (d) $m(1 + 1/k) - 1$ (e) $m(1 - 1/k) - 1$.

2. Solutions

#1367: *Proposed by Thomas Garrity, Steven J. Miller and Chenyang Sun (Williams College).*
We say a positive integer is a side-into-hypothesis number if it is both a side of a right triangle with integer lengths and the hypotenuse of a triangle with integer sides. Thus 5 is such a number, from the 3–4–5 triangle and the 5–12–13.
(a) Prove or disprove: there are infinitely many side-into-hypothesis numbers.

(b) Prove or disprove: there exists an infinite sequence of positive integers $\{x_n\}$ such that x_n is a side of a right triangle with x_{n+1} as a hypotenuse.

Solution by ***David E. Manes, Oneonta, NY****. Also solved by the* ***Skidmore College Problem Group****.*

Note that for each positive integer n, $(5n)^2 + (12n)^2 = (13n)^2$ and $(3n)^2 + (4n)^2 = (5n)^2$. Thus the integer $5n$ is a side - into - hypothesis number since it is a side in the $5n - 12n - 13n$ right triangle and the hypotenuse in the $3n - 4n - 5n$ triangle. Therefore, there are infinitely many side - into - hypothesis numbers.

For part (b) define the sequence $\{x_n\}$ such that $x_1 = 3$, $x_2 = 5$ and for $n \geq 3$,

$$x_n = (x_{n-1} - 1)\left(\frac{x_{n-1} + 1}{2}\right) + 1.$$

We will show that each x_n is the side of a right triangle with hypotenuse x_{n+1}. More precisely, we will show that $x_n^2 + (x_{n+1} - 1)^2 = x_{n+1}^2$. Note that the sides $(x_n, x_{n+1} - 1, x_{n+1})$ do define a triangle for each $n \geq 1$. Moreover, by the given example, the result is true for $n = 1$ and $n = 2$. Assume inductively that the result is true for any integer $n \geq 2$. Then

$$\begin{aligned} x_{n+1}^2 + (x_{n+2} - 1)^2 &= x_{n+1}^2 + x_{n+2}^2 - 2x_{n+2} + 1 \\ &= x_{n+1}^2 + x_{n+2}^2 - 2\left[(x_{n+1} - 1)\left(\frac{x_{n+1} + 1}{2}\right) + 1\right] + 1 \\ &= x_{n+1}^2 + x_{n+2}^2 - x_{n+1}^2 + 1 - 2 + 1 \\ &= x_{n+2}^2. \end{aligned}$$

Therefore, the result is true for $n+1$ and so by induction each x_n is the side of a right triangle with integer sides $(x_n, x_{n+1} - 1, x_{n+1})$ and hypotenuse x_{n+1}. This completes the solution.

GRE Practice #6: The following is essentially the famous German Tank Problem. There are N tanks, labeled $1, 2, \ldots, N$, and k distinct serial numbers $s_1, s_2, \ldots, s_k$ are observed, with $m = \max s_i$ the largest value. If every subset of size k is equally likely, what is the best predictor for N as a function of m and k?
(a) mk (b) $m(1 + 1/k)$ (c) $m(1 - 1/k)$ (d) $m(1 + 1/k) - 1$ (e) $m(1 - 1/k) - 1$.

While this problem can be solved through combinatorial manipulations, that is time consuming. Instead, let us look at extreme cases and eliminate four of the five answers.

First, (a) is clearly out as if k is large than m will be large (if $k \geq N/2$ then $m \geq N/2$), and thus mk will exceed N!

We now come to four answers that are very similar. If we take the special case $k = N$ then $m = N$ (every tank is observed) and thus our prediction should be N. The answers we get in this special case are $N + 1$ for (b), $N - 1$ for (c), N for (d) and $N - 2$ for (e), which suggests (d) as the answer.

We could also look at $k = 1$ to gain some reasonableness. Note that we will never guess less than m for the number of tanks, so it makes sense to look at a guess of the form $m + g(m, k)$ for some function g. As m increases we should predict a higher value of N, so it makes sense that g is increasing with m. Similarly, if k increases then we've observed more tanks and we're more confident that the largest observed serial number is close to N, and thus the boost should be decreasing with k. This leads to guessing $g(m, k) = \alpha m/k + \beta$; the answer turns out to be $\alpha = -\beta = 1$. Returning to taking $k = 1$, it's likely that our observed m is around $N/2$, so we would want to double it. While this eliminates (c) and (e), both (b) and (d) survive (which is not surprising, as they differ by a constant).

This problem is an excellent example of the power of spending some time thinking about a problem and getting a feel for the answer.

Email address: sjm1@williams.edu

Professor of Mathematics, Department of Mathematics and Statistics, Williams College, Williamstown, MA 01267